U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

December 11, 2020

BY ECF
The Honorable William H. Pauley III
United States District Judge
Southern District of New York
500 Pearl Street
New York, New York 10007

Re: *United States v. Michael R. Weigand*, 20 Cr. 510 (WHP)

Dear Judge Pauley:

The Government respectfully submits this letter in advance of sentencing in the above-captioned case, which is scheduled for December 18, 2020, at 2:00 p.m. In September 2020, defendant Michael R. Weigand (the "defendant" or "Weigand") pleaded guilty, pursuant to a plea agreement with the Government (the "Plea Agreement"), to making false statements about, among other things, his involvement in the Silk Road website. Pursuant to the Plea Agreement, the applicable range under the U.S. Sentencing Guidelines ("Guidelines" or "U.S.S.G.") is 6 to 12 months' imprisonment (the "Stipulated Guidelines Range"). For the reasons set forth below, the Government respectfully submits that a sentence at the top of that range is warranted in this case.

I. FACTUAL BACKGROUND

A. Overview

From January 2011 until October 2, 2013, the Silk Road website hosted a sprawling black-market bazaar on the Internet, where illegal drugs and other illicit goods and services were bought and sold by the site's users. Silk Road was used by several thousand unlawful vendors to distribute hundreds of kilograms of illegal drugs and other illicit goods and services to over 100,000 buyers, and to launder hundreds of millions of dollars derived from these unlawful transactions. In total, approximately $183 million dollars' worth of illegal drugs were sold on Silk Road. Silk Road was the most sophisticated criminal marketplace on the Internet at the time. The creator, owner, and operator of Silk Road was Ross William Ulbricht, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road." Ulbricht's senior adviser was Roger Thomas Clark, whose online nicknames included "Variety Jones," "VJ," "Cimon," and "Plural of Mongoose."

Defendant Michael Weigand's misconduct spans from 2011 to 2019 and has several dimensions. Weigand's misconduct includes (1) participating in Silk Road, including by providing technological advice to Clark and Ulbricht; (2) laundering more than $75,000 worth of Silk Road proceeds after the website was shut down by law enforcement; and (3) obstructing the Government's investigation of Silk Road in multiple ways after the site was shut down, such as (a) removing Silk Road evidence from Clark's apartment in London, (b) spreading disinformation, and (c) lying repeatedly during an interview with law enforcement.

B. Overview of the Silk Road Website

Silk Road was an extensive and sophisticated online criminal marketplace. It sought to make conducting illegal transactions on the Internet as easy as shopping online at mainstream websites. Silk Road offered a sales platform that allowed users to conduct transactions online, and the basic user interface resembled those of typical online e-commerce marketplaces. The only form of payment accepted on Silk Road was Bitcoin, an electronic currency that exists only on the Internet and not in any physical form. (U.S. Probation Office's final PSR (Dkt. 8) at ¶¶ 10, 13).

The Tor Network: Unlike mainstream e-commerce websites, Silk Road was only accessible on the Tor network—a special network of computers that is designed to conceal the true Internet Protocol (or "IP") addresses of the computers on the network and, thereby, the identities of the network's users. Every communication sent through Tor is bounced through relays within the network, and wrapped in layers of encryption, such that it is practically impossible to trace the communication back to its true originating IP address.[1] (*Id.* ¶ 11).

Silk Road User Interface: Upon arriving at the Silk Road website, a user entered his username and password. The user was then directed to Silk Road's homepage, which included a "Shop by Category" list, with links to various categories of illegal items for sale on the site, including "Drugs." The homepage also contained photographs of certain listings on the site. When a user clicked on an item for sale, the website would bring up a page with information about the item (*e.g.*, a description of the item, its price, and prior reviews of the product). To buy an item, the user simply clicked on a link to add the item to an electronic "shopping cart." The homepage also included links to: (1) a private message system, which allowed users to send messages to each other through the site; (2) online forums, where users could post messages to "discussion threads"; (3) a "wiki," which contained a collection of frequently asked questions; and (4) a "customer service" section, where users could get support from the Silk Road administrative staff. (*Id.* ¶ 15).

Illegal Goods and Services Sold: The illegal nature of the items sold on Silk Road was readily apparent. The vast majority consisted of illegal drugs of nearly every variety, which were openly advertised as such and were visible on the site's homepage. As of the takedown of the Silk Road website on October 2, 2013, there were about 13,802 listings for controlled substances on the site, listed under categories such as "Ecstasy," "Opioids," "Prescription," and "Psychedelics." Silk Road also offered for sale counterfeit and fraudulent identity documents, including counterfeit U.S. and foreign passports and drivers' licenses. As of October 2, 2013, Silk Road had about 156 listings for forged identity documents. Silk Road also offered a wide variety of computer hacking tools. As of October 2, 2013, Silk Road offered the following computer hacking goods: (1) account password hacking tools and services, which included tools for compromising the usernames and passwords of victims' electronic accounts, including email and Facebook accounts; (2) Remote Access Tools ("RATs"), which facilitate unauthorized remote access to a compromised computer, including webcam activity; and (3) keyloggers, which allow a user to monitor keystrokes inputted by a victim into his computer, used to steal confidential information. Finally, Silk Road offered a

[1] An IP address is functionally similar to a street address or a phone number—it is how devices communicate with each other over a network and, in the absence of Tor, it can be used to identify the user and location of the device.

variety of money laundering services to its users (*e.g.*, cash, anonymous debit cards preloaded with currency, etc.). Many of these money laundering services were marketed to Silk Road vendors as a means to convert their Bitcoin proceeds into other forms of currency. (*Id.* ¶ 25).

Volume of Illegal Transactions on Silk Road: In total, Silk Road had approximately 3,748 registered vendor accounts and 115,391 registered buyer accounts. About 1.5 million transactions occurred over Silk Road, with a total of value of approximately $213.9 million in United States currency. These transactions generated a total of about $13.2 million in commissions for Silk Road. Sales of illegal narcotics accounted for about $183 million (of the $213 million), including:

	Number of Sales	Quantity (kg)	Total Sales Revenue
Heroin	53,649	26.8	$8,930,657
Cocaine	82,582	82.6	$17,386,917
Methamphetamine	34,689	8.7	$8,110,453
LSD	54,567		$7,073,838

There were also more than $1 million in sales of counterfeit identity documents, and more than $3 million in sales of money laundering-related services. (*See id.* ¶ 19).

C. Ross Ulbricht's Arrest and Roger Thomas Clark's Roles in Silk Road

On October 1, 2013, Ross Ulbricht was arrested at a public library in San Francisco. Agents seized Ulbricht's laptop computer, while it was open; Ulbricht was logged in to Silk Road under the username "Dread Pirate Roberts." (*Id.* ¶ 16). Subsequent examination of Ulbricht's computer revealed a significant volume of evidence tying him to the creation, ownership, and operation of Silk Road for the entire period of its existence. This included, among other things:

- Thousands of pages of chat logs with co-conspirators, including Roger Thomas Clark;
- Journal entries describing Ulbricht's ownership and operation of Silk Road;
- A copy of the Silk Road website, and a copy of a Silk Road–related database, including information regarding Silk Road users and transactions; and
- Scanned copies of identification documents belonging to members of Ulbricht's very small Silk Road staff, including Roger Thomas Clark's Canadian Passport.

(*Id.* ¶ 17). Shortly after Ulbricht's arrest, law enforcement placed a "banner" on the Silk Road homepage, stating that the site had been taken down by the FBI. (*Id.* ¶ 18).

The information on Ulbricht's computer also revealed that his lead partner in crime was Clark. Clark's central roles in Silk Road included (1) advising Ulbricht about security, technology, promotions, and the rules that governed Silk Road users; (2) devising a "cover story" to make it appear that Ulbricht had sold Silk Road; (3) hiring a programmer to improve the infrastructure of, and maintain, Silk Road; (4) gathering information on law enforcement's efforts to investigate Silk Road; (5) investigating a Silk Road employee's disappearance; and (6) protecting the Silk Road enterprise, including urging and facilitating an attempted murder-for-hire of a Silk Road employee suspected of stealing $350,000 from the site. (*See* 15 Cr. 866 (WHP), Dkt. 64, at pp. 8-16).

D. Weigand's Misconduct

As explained below, Weigand's misconduct includes (1) participating in Silk Road, including by providing technological advice to Clark and Ulbricht; (2) laundering about $75,000 worth of Silk Road proceeds after the site was shut down by law enforcement; and (3) obstructing the Government's investigation of Silk Road in multiple ways, such as (a) removing Silk Road evidence from Clark's London apartment, (b) spreading disinformation, and (c) lying repeatedly during an interview with law enforcement.[2] (*Id.* ¶ 21).

1. Weigand's Participation in Silk Road

a. Weigand and Clark Join Silk Road

Weigand and Clark knew each other from working together in the marijuana seeds business. On June 27, 2011, "Shabang" and "Variety Jones" (*i.e.*, Weigand and Clark) both joined Silk Road, about 50 minutes apart. In September and October 2011, "Shabang" and "Variety Jones" both purchased "vending" privileges on Silk Road, which permitted both accounts to sell items on Silk Road. (*Id.* ¶ 22).

On September 30, 2011, about 42 Bitcoin was sent directly from a cryptocurrency account to the "Shabang" account on Silk Road. (In order to buy anything on Silk Road, a user needed Bitcoin in their Silk Road account; it was therefore necessary to send Bitcoin to one's Silk Road account.) Thus, in this case, funds were sent directly from a particular cryptocurrency exchange account into the "Shabang" account on Silk Road. That cryptocurrency exchange account (the "Weigand Crypto Account-1") is associated with Weigand's name, date of birth, residential address, a scanned color copy of his Ohio State Driver's License (including his photograph), and an Ohio State tax form addressed to Weigand and his spouse. (*Id.* ¶ 23).

On two occasions in October 2011, Clark's Silk Road account ("Variety Jones") was funded by Bitcoin which traced to Bitcoin transactions involving the Weigand Crypto Account-1. (*Id.* ¶ 24).

b. Clark Describes His Close Relationship with Weigand

To understand Weigand's misconduct, it is necessary to understand how close Weigand and Clark were (and perhaps still are). In chats with Ulbricht,[3] which were recovered from Ulbricht's computer, Clark described several dimensions of his close relationship with Weigand. *First*, Clark indicated that he worked very closely with "~s".[4] For example:

---

[2] For avoidance of doubt, the Government is using the term obstruction in a general sense. By its plain terms, U.S.S.G. § 3C1.1 (a sentencing enhancement for obstruction of justice) does *not* apply here.

[3] All chat logs are quoted verbatim, including any errors in spelling, grammar, and punctuation.

[4] Weigand was referred to, by Clark and Ulbricht, as "shabang," "~shabang~," "~s," or "s".

- On or about June 12, 2012, Clark wrote to Ulbricht, in substance and in part (emphasis added): "**~s has a piece of everything I do, becuase I have the same from him.** He's the guy to get our forum going, but he's not in the top circle, cause he doesn't want to be, he wants to raise a family without the high level of stress. He's a resource, and a great one, but doesn't want to go all in." (*Id.* ¶ 26).

- On or about December 7, 2011, Clark wrote to Ulbricht, in substance and in part, "when we started (~S and I) on tracking SR, it was with the intention of wiping ya' off the face of the earth, and dancing upon yer graves."

- On or about December 22, 2011, Clark wrote to Ulbricht, in substance and in part, "Could you please change Shabangs name from Shabang to ~shabang~ please. He's been bugging me to ask for about 2 weeks, and I keep forgetting. He'd love it if you still didn't allow anyone else to have tilde's in their name. kind of his trademark, and why we call him ~s."

- On or about December 27, 2011, Clark wrote to Ulbricht, in substance and in part (emphasis added), "**you, me, ~S - that's my circle of trust for this** - anyone else - DA, nb, etc, they are close, but not in."

- On or about January 21, 2012, Clark wrote to Ulbricht, "Tex is a fucking star – wouldn't be doing this if I didn't have him to do the back end. * * * couldn't do without ~s, and yer certainly pretty fucking critical to my way of thinking nowadays. Always looking out for good people, at any level."

Second, in chats with Ulbricht, Clark made clear that he (Clark) was not an expert programmer, but "~s" was. For example, on or about December 7, 2011, Clark wrote to Ulbricht, in substance and in part, "I'm not a specialist - I'm kinda like you - I know you haven't got extensive experience doing what you do." On the same day, Clark also wrote to Ulbricht that, "~s is a PHP expert".[5] On the same day, Clark also told Ulbricht, "my speciality is marketing." On the same day, Clark also wrote to Ulbricht, in substance and in part, "I know fuck all about the workings of Tor - or didn't - but I've read the source code, stared at fucking whiteboards, and **spent hundreds of h ours working with S who has been running dope on a hidden service since Nov 2006 - just over 5 years**" (emphasis added).

Third, Clark explained to Ulbricht that he (Clark) and "~S" hacked the Silk Road website three times because, before getting more involved in the site, they wanted to see if Ulbricht was saving users' information, which would endanger users' anonymity and liberty. For example, on or about December 7, 2011, Clark wrote to Ulbricht, in substance and in part (emphasis added):

> sometime, I'm gonna hafta bite the bullet and tell you / like **the 3 times we romped about in your sites** * * * we didn't know whether or not we could trust you way back then. * * * by trust, I mean we wanted to know wheter or not you were doing what we'd call bad things / saving info you shouldn't

[5] PHP is a general-purpose programming language designed for web development.

> * * * were addresses really deleted, or did you save them away for a rainy day * * * I couldn't get in SR after a couple days of trying, so we switched, and I pentrated the forums * * * **~S went after SR, and in two days got in for a look**. * * * and we want you to know we only did it that time because, like we said, it's in our best interests for you to survive, and we were worried you did not have control of your forums, at a minimum

(*Id.* ¶¶ 28-29). On the same day, Clark wrote to Ulbricht, in substance and in part, "Sorry, tied up for a sec texting ~S / He says – tell him [*i.e.*, Ulbricht] we don't have his IP from our travels. Also tell him that he should assume anyone that was in there has his IPS."

Clark and Weigand thus spotted a key vulnerability at a somewhat early stage of Silk Road's development. This allowed Ulbricht to improve his security. More broadly, Clark and Weigand's hack of Silk Road proved to Ulbricht that they had real value, since technology and security were pivotal to Ulbricht, and Ulbricht was a novice in this space. Clark and Weigand's hack also appears to be at least part of what gave Clark an "in" with Ulbricht; Clark leveraged this opening. With the benefit of hindsight, this opening—created by Clark and Weigand's hack—proved important; Clark's teaming up with Ulbricht ultimately helped transform Silk Road.

Fourth, Clark and "Shabang" believed that Silk Road could be useful to them in the marijuana seed business. (*Id.* ¶ 28). For example, on or about December 7, 2011, Clark wrote to Ulbricht, in substance and in part:

> so that's what I mean when we say we just want to do cannabis - we want to do all the cannabis. * * * we'd like to do a canabis only site - and personal amounts only as well - 1/4oz kinda things. * * * want over 1/4oz, or want some coke with that - go to SR. * * * so we dont want to compete, per se - we believe a rising tide raises all ships. but in a few months when we launch, we'd like to have a tight relatinship with you, as well as know that you're safe and can expand. * * * and that's why we've been keeping an eye on you, and slipping into yer kitchen a couple of times.

Fifth, Clark and "Shabang" worked on technology and securing servers effectively. For example, on or about December 7, 2011, Clark wrote to Ulbricht, in substance and in part, "once we're sure you're platform is stable, we'll show you how to make it so your server is just a box, with nothing to lose on it." On the same day, Clark also wrote to Ulbricht, in substance and in part (emphasis added), "**S would like you to recall that he also pm'd** [*i.e.*, private messaged] **you when SR was down to tell you it was your version of Tor not meshing with the v2 desriptors**." Clark added, on the same day, "**that's the reason we're working with you first to harden your systems.** When we're done, even getting the server will give them nothing."

Sixth, "Shabang" supplied Clark with advice, technological analysis, ideas, and notes. For example, on or about December 6, 2011, Clark wrote to Ulbricht, in substance and in part (emphasis added): "ha - sorry - was looking at shabangs notes on his, meant to paste that in the text editor I'm using keeping track of this / he wrote his in C and I'm just looking at the source to see how he handled socks bindin." In addition, on or about January 3, 2012, Ulbricht asked Clark,

in substance and in part, whether a particular technique "effectively negate[s] any known cold-boot attack vector," and during the course of his reply, Clark wrote, in substance and in part, "~s would also like it known that a 'cold boot' is a specific term that refers to restarting a processor by interrupt without removing power. Frigid boot attack is the proper nomenclature." And on or about April 13, 2012, Clark wrote to Ulbricht: "Oh, had a lonnnng chat with ~s and the frigid boot team today. Gving them 10 more days, as 4.20 stuff and Smed are gonna keep me tied up anyways, so it's not like I've got time to work on forum stuff with ~s. Also, I'm geting him to set up the forum demo / chat server that I said I'd do this week and didn't".

Seventh, Clark told Ulbricht that he (Clark) and "Shabang" had set up a shell of a website in furtherance of their work together, and Clark provided the link to that site. Website domain registration information showed that Weigand had registered this site—along with many others.[6]

In sum, Clark and Weigand had an extremely close working relationship.

c. Weigand Supplied Technological Advice Directly to Ulbricht

"Shabang" also directly messaged with Ulbricht—both on the Silk Road Forum and in private messages—regarding technological advice. (*Id.* ¶ 27). (At that time, Ulbricht was using the moniker, "Silk Road.") On or about December 1, 2011, "Shabang" responded to "Silk Road"'s Forum post by stating, in substance and in part:

> It's not possible for any node to block traffic for a specific hidden service address as no node is aware that it is carrying traffic for a specific hidden service address, or the whole system wouldn't be anonymous. * * * Your problem is your guard nodes are not set up in a fashion suitable for a hidden service serving at the volume you are. The URL change will help in the very short term, as the new guard nodes will be fresh, but will be adding clients at a rapid clip, and the 'blocking' problem will arise again.
>
> You are throwing the wrong solution at the wrong problem, and executing it poorly as well.

"Silk Road" (*i.e.*, Ulbricht) then replied to "Shabang," "Criticism accepted, couldn't agree more. I've sent you a pm [*i.e.*, a private message] regarding the guard node issue."

On or about the same day, "Shabang" sent or received several private messages on the Silk Road Forum, including three with "Silk Road" (*i.e.*, Ulbricht) (emphasis added):

- **Silk Road to Shabang**: "Thanks for the criticism and advise. I wasn't sure that was the problem, but it was getting untenable. **Can you please explain in further**

[6] Indeed, between 2011 and 2014, Weigand registered about 25 domains that reference Bitcoin, Tor, or cannabis/seeds/THC/marijuana/weed, including at least one that refers to Silk Road. (PSR ¶ 30). (A "domain name" is a simple, easy-to-remember way for humans to identify computers on the Internet. For example, "www.usdoj.gov" and "www.yahoo.com" are domain names.)

detail the issue you think it is with the guard nodes, and how to set things up properly? I can pay you for your time. And why is it that using a fresh url works in the short term?"

- **Shabang to Silk Road**: "I'm sorry for getting angry, **I think you've been getting bad advice, and VJ and I have been talking for weeks what to do about it.** * * * I do want to lecture you, but I shouldn't have done it in the thread.

  We really need to set up a secure 3-way chat, because there's far too much to explain in messages back and forth if you're not sure the recipient got the first point, the rest of the message is lost. I'll email VJ and get him to set it up with you.

  The new url works because you're seen as a new service, so suitable guard nodes are searched for using metrics of uptime (8 days plus), not flagged as a bad exit, and above a certain calculated bandwidth. **New guard nodes are at the top of your list, and Tor keeps track of several for you.** Each time you start up, it picks one from the list, and new ones arent' picked for months.

  It's expected that a guard node would get a client that carries traffic orders of magnitude less than yours, so it doesn't reserve you bandwidth you need, and packs on new nodes as they request guard nodes. The nodes get congested, but Tor doesn't drop them for congestion, just if they don't respond at all.

  So your site gets slower.

  Don't bother to offer VJ or I payment for our time, you really can't afford us. That little exploit we've found that could expose your server that we still have to get around to patching for you - there is no way that with a little shopping around that would be worth less than $100,000 instantly. * * *

  We're going to work with you because we both make a lot of money in the cannabis business, we see hidden services and bitcoins as the greatest web opportunity since search, and we are worried that if you get shut down, it will kill both bicoins - yes you could take them down - and any chance of there being a viable, vibrant, public venue for our wares.

  In short, what's good for you is good for us.

  ~shabang~"

- **Silk Road to Shabang**: "**Feel free to lecture me** through pm (I check the main site pm's more often) or I'll wait to hear from you regarding real-time chat. **Thank you for your help**."

In these online conversations, "Shabang" told Ulbricht, among other things, that (1) "VJ" and "Shabang" work together ("*I think you've been getting bad advice, and VJ and I have been*

talking for weeks what to do about it."; "*Don't bother to offer VJ or I payment for our time, you really can't afford us.*"); (2) "VJ" and "Shabang" identified a vulnerability in the Silk Road website ("*That little exploit we've found that could expose your server that we still have to get around to patching for you*"); and (3) "VJ" and "Shabang" are "going to work with" Ulbricht because they "see hidden services and bitcoin as" a great opportunity—an opportunity they could lose were Silk Road to get "shut down." (*Id.*).

Thus, as Clark had told Ulbricht, Weigand was "a resource, and a great one," but did not want to go "all in" like Clark and Ulbricht. Weigand was not a Silk Road employee, but once the site was shut down, he took several steps to obstruct the Government's investigation. These steps are discussed next.

2. Weigand Travels to Clark's London Apartment and Removes Silk Road Evidence

In October 2013, the Government arrested Ulbricht in San Francisco and shut down the Silk Road website. At Ulbricht's SDNY bail hearing on or about November 21, 2013, the Government publicly disclosed—for the first time—that it had been able to access the contents of Ulbricht's laptop. This was extremely consequential. Ulbricht's laptop contained scanned color copies of his employees' IDs, including Clark's passport. Ulbricht's laptop therefore identified his employees and his right-hand man, Clark.[7] Ulbricht's seized electronics included communications with Clark and Weigand, including chats with Clark about YubiKeys.[8] (*Id.* ¶ 31).

Several hours later on November 21, 2013, about 28 Bitcoins (worth more than $20,000 at the time) were deposited into Weigand Crypto Account-1. These Bitcoins were traceable to "Variety Jones"'s Silk Road account, and further traceable to an August 2013 payment Ulbricht had made to "Variety Jones." Thus, Clark paid Weigand more than $20,000 (in Bitcoin) mere hours after the Government disclosed it had been able to access the contents of Ulbricht's laptop. (*Id.* ¶ 32).

On November 24, 2013—only three days after this revelation—a trip was booked from Cleveland to London in Weigand's name, but using the credit card of Weigand's relative, whose first name differs. Travel records reveal that the dates of Weigand's trip were November 30, 2013 until around December 7, 2013—*i.e.*, Weigand traveled to London less than one week after this trip was booked. In addition, Weigand flew through Toronto on his trip to and from London. (*Id.* ¶ 33). Thus, Weigand's trip was suddenly planned, paid for by a relative, arranged so that it might appear to U.S. border authorities as a trip to Canada, and taken by a man who rarely traveled abroad. (From 1995 through 2018, Weigand had only approximately ten known border crossings, including border crossings in both directions for this 2013 trip to London.)

---

[7] Within a month of this disclosure, the Government, aided by this identity evidence, charged several members of Ulbricht's small staff. *See United States v. Jones et al.*, 13 Cr. 950 (JMF), Dkt. 3 (S1 Indictment dated 12/19/2013).

[8] A YubiKey is a hardware authentication device that uses two-factor authentication; like Bitcoin and Tor, YubiKeys are not inherently illegal. (PSR ¶ 34).

Weigand removed YubiKeys from Clark's apartment in London during late 2013. CW-1 had previously purchased thousands of dollars' worth of YubiKeys at Clark's request, had kept about 200, and had given the remainder to Clark in London.[9] Indeed, during their chats, Clark and Ulbricht repeatedly discussed YubiKeys; the term "YubiKey" appears in their chats more than 180 times. On or about April 17, 2012, for instance, Clark messaged Ulbricht, "The first yubikeys have arrived in London!" When Ulbricht asked if this batch consisted of 500 YubiKeys, Clark confirmed that it did. Clark also facilitated the sale of YubiKeys on Silk Road. Thus, as of fall 2013, the very large quantity of YubiKeys in Clark's apartment in London were very important evidence; they constituted physical evidence that corroborated the online communications. And they concerned a piece of hardware that is not common knowledge. The YubiKeys in Clark's London apartment therefore helped demonstrate that (1) the chats on Ulbricht's laptop were not merely talk; and (2) "Variety Jones," who had repeatedly chatted about YubiKeys, was indeed Clark. These facts presumably informed Clark's decision to send someone extremely trusted to his London apartment promptly—even if they were an ocean away.[10] (*Id.* ¶ 34).

3. Weigand Laundered Silk Road Proceeds After the Website Was Shut Down

After Silk Road was shut down, Weigand laundered Silk Road proceeds in two ways—(1) Silk Road Bitcoin, and (2) YubiKeys purchased with Silk Road proceeds.

Silk Road Bitcoin: In 2013 and 2014, Weigand laundered Silk Road proceeds. Specifically, in August 2013 (before Silk Road was shut down), Ulbricht paid Clark by depositing 415 Bitcoin in Clark's account on Silk Road. Clark sent more than 80 of those Bitcoin to Weigand. Between in or around November 2013 and June 2014, Weigand funneled these Bitcoin through multiple accounts and Bitcoin exchanges. Ultimately, Weigand sent these funds, through Bitcoin exchanges based in Japan and Luxembourg, to a bank account he controlled in Ohio. In total, during this period, Weigand laundered at least about $65,702.37 in Silk Road Bitcoin. (*Id.* ¶ 36).

YubiKeys: The YubiKeys that Weigand removed from Clark's London apartment had been purchased with Silk Road proceeds, as evidenced by an accounting spreadsheet on Ulbricht's laptop, Bitcoin transfers between Ulbricht and Clark, and an invoice showing payment by CW-1 for YubiKeys. After removing these YubiKeys from Clark's apartment, Weigand cleaned these YubiKeys—and converted them to currency—by selling at least hundreds of them on an online auction website starting in early 2014. Weigand sold these YubiKeys for more than $10,000 in total. (*Id.* ¶ 35). Weigand's combined laundered amount, which exceeds $75,000, is the loss amount stipulated in the Plea Agreement. (*Id.* ¶¶ 4, 21, 54).

---

[9] CW-1 was a Silk Road programmer who worked directly with Clark and Ulbricht; CW-1 even lived with Clark in Thailand during some of the period of Silk Road.

[10] Clark was charged and arrested in 2015. As of November 2013, Clark was living in Thailand. As noted, Clark's true identity was revealed by Ulbricht's laptop. It is reasonable to infer that Clark concluded that, if he traveled to the U.K., he would have been arrested; so Clark's partner, Weigand, went instead. Weigand's passport was *not* on Ulbricht's laptop—unlike the passports/IDs of Clark and of Ulbricht's everyday employees.

4. Weigand and Clark Spread Disinformation in an Attempt to Discredit the Government's Silk Road Investigation

On September 10, 2015, *Motherboard* published an article identifying Clark as "Variety Jones," an architect of Silk Road. This appears to have been the first time that Clark was publicly identified. Over the next month, Clark and Weigand engaged in a coordinated disinformation campaign. Clark's apparent goal, with Weigand's assistance, was to try to plant the seeds of his criminal defense by focusing attention on allegedly corrupt law enforcement and the purported unreliability of electronic evidence—like the evidence on Ulbricht's computer that had helped identify Clark. A key piece of Clark's strategy was to claim that a corrupt FBI agent was allegedly hunting/threatening Clark through messages on TorChat.[11] This culminated in a September 27, 2015 post, by Clark, on a marijuana forum called MyPlanetGanja (described in detail below).

One problem with this outlandish, baseless claim was that Clark claimed to be receiving threats on a chat program that he didn't even have. Clark needed Weigand's help in order to access the version of TorChat required for Clark's forthcoming story about the purportedly rogue FBI agent. Thus, one day before Clark's post about this purported agent, Clark posted on the same marijuana forum seeking Weigand's help. (Clark technically directed his post to "Chester"; in a 2018 interview with law enforcement, Weigand confirmed that he was "Chester.") In his post, Clark asked for "a favor," and explained that a particular version of TorChat ("Old 0.9.9.553") "won't work without a little tweaking." Clark therefore asked Weigand, "Would it be asking too much for ya' to write up a little guide on how to do aforesaid tweakin' in laymans terms"?

Weigand (as "Chester") promptly replied on MyPlanetGanja. Weigand wrote, in part, "Dude, do you have ANY idea how long it would take to write that up in detail with the requisite screen shots??" Weigand explained that the "tor network has seen several major updates since TorChat version 0.9.9.553." Weigand noted that there was "another path however," and he supplied basic instructions and a link, coderodentjy677u.onion.[12] Clark promptly replied, "Thanks for posting that up there Chester . . . [a]nd thank you everyone else for your patience. That post of mine you've been waiting for, will be my next post."

Armed with Weigand's insight about this old version of TorChat, Clark promptly posted, less than 24 hours later, his unfounded attack on the integrity on the Government's investigation. In his post, Clark claimed that a rogue FBI agent, "Diamond," was threatening him. Clark alleged that a "highly placed member" of the FBI, "Diamond," was leaking grand jury information and blackmailing dark web marketplace owners. Clark alleged that this "bent Federale" had "looted" Ulbricht's Bitcoin from Silk Road and thereby acquired a Bitcoin wallet with more than 300,000 Bitcoin, which was worth more than $75 million. According to Clark, "Diamond" had also threatened to torture Ulbricht's relatives. So, Clark wrote, he was turning himself in, because a corrupt FBI agent was hunting him and Clark feared for his life. Clark's allegations were baseless. Yet Weigand helped Clark to spread disinformation to try to aid them both and discredit the

[11] TorChat is an anonymous, encrypted instant messenger program that uses Tor.

[12] Weigand's signature block included the following quote: "LAW - The tool used by government to control it's [sic] citizens (current US definition)."

Government's investigation. For instance, on another online forum, Weigand's posts at this time spread disinformation about the integrity of the electronic evidence on Ulbricht's computer—evidence that helped identify both Clark and Weigand. Weigand also parroted Clark's language, writing of purportedly "bent feds" in a post. Thus, right after Clark was publicly identified, Clark and Weigand engaged in a coordinated disinformation campaign focusing on allegedly corrupt law enforcement and the purported unreliability of electronic evidence. (*Id.* ¶¶ 38-44).

5. Weigand's False Statements

In January 2019, Weigand again engaged in obstructive conduct to try to protect Clark and himself. At that time, Weigand was questioned by Special Agents from the IRS and the FBI.[13] After being specifically warned that it is a federal crime to make a false statement to a federal law enforcement officer, Weigand attempted to cover up his involvement in Silk Road by falsely stating, among other things, that (1) he never opened an account on Silk Road; (2) he never used the online pseudonyms "Shabang" or "~Shabang~"; (3) he never transferred Bitcoin to Silk Road; (4) he never exposed computer security vulnerabilities in the Silk Road website; (5) he never communicated with anyone who used the online pseudonym "Dread Pirate Roberts," "DPR," or "Silk Road"; (6) he never performed any services for the Silk Road website; (7) he did not know the true identity of "Variety Jones" on Silk Road; and (8) he used the aforementioned Bitcoin exchange in Japan (*i.e.*, Cryptocurrency Exchange-1) only for mined Bitcoin.[14] Weigand also falsely stated that the purpose of his trip to London in late 2013, following the takedown of the Silk Road website and arrest of Ulbricht, was to meet with Clark's associate regarding a marijuana seed business. In fact, as noted, Weigand traveled to Clark's London residence and removed Silk Road evidence (YubiKeys). Weigand thus lied in at least nine different respects. (*Id.* ¶¶ 45-46).

II. PROCEDURAL HISTORY

On September 21, 2020, Weigand surrendered and pleaded guilty before Your Honor to a one-count Information charging him with false statements in violation of 18 U.S.C. § 1001. (Dkt. 2). On December 4, 2020, the defense filed its sentencing submission, requesting a sentence of time served. (Dkt. 6 ("Def. Mem.")). On December 11, 2020, Probation issued the final PSR (Dkt. 8), recommending a sentence of 6 months' imprisonment and 3 years of supervised release.

III. APPLICABLE LAW

As the Court is well aware, "a district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range," which is "the starting point and the initial

[13] At the time of this meeting, the statute of limitations had not run as to at least some of Weigand's Silk Road–related offenses. For instance, Weigand's money laundering extended into at least mid-2014, and thus, the statute of limitations had not run as of January 2019.

[14] Bitcoin mining is essentially a process whereby bitcoin "miners" use computer hardware to perform mathematical functions which ensure that transactions are properly recorded in Bitcoin's "Blockchain," or public ledger. As a reward for this work, miners are paid any transaction fees associated with the transactions they process, as well as a subsidy of newly created coins.

benchmark. The Guidelines are not the only consideration, however." *Gall v. United States*, 552 U.S. 38, 49 (2007). Rather, "after giving both parties an opportunity to argue for whatever sentence they deem appropriate, the district judge should then consider all of the § 3553(a) factors to determine whether they support the sentence requested by a party." *Id.* The seven factors outlined in 18 U.S.C. § 3553(a) include the nature and circumstances of the offense, the need to adequately deter criminal conduct and promote respect for the law, the need to protect the public from further crimes of the defendant, and the need to avoid unwarranted sentencing disparities. *Id.* at 50 & n.6. When considering these factors, the judge "may not presume that the Guidelines range is reasonable. He must make an individualized assessment based on the facts presented." *Id.* at 49–50. If the judge "decides that an outside-Guidelines sentence is warranted, he must consider the extent of the deviation and ensure that the justification is sufficiently compelling to support the degree of the variance . . . . [A] major departure should be supported by a more significant justification than a minor one." *Id.* at 50.

IV. DISCUSSION

The Government respectfully submits that a top-of-the-Guidelines sentence is warranted in this case, principally in light of the nature, seriousness, harmfulness, and deceptiveness of the offense; the need for just punishment and promoting respect for the law; and the need for deterrence.

First, as to the nature and circumstances of the offense, Weigand's misconduct was extremely serious. After aiding Silk Road's principals, and then laundering Silk Road proceeds, Weigand waged a sustained campaign to obstruct the Government's Silk Road investigation. This obstructive campaign was at least partially coordinated with Clark, as is evidenced by Weigand's sudden trip to London to retrieve Silk Road evidence from Clark's apartment, Clark's transferring more than $20,000 in Bitcoin to Weigand right before that trip, and Weigand and Clark's nearly simultaneous posts spreading disinformation right after Clark was publicly identified for the first time. This obstructive campaign culminated in Weigand's repeated, widespread lies to law enforcement in 2019, including about whether he and Clark were involved in Silk Road. Weigand's lies were not a spur-of-the-moment crime. In November 2018, agents approached Weigand in Ohio and interviewed him. Then, Weigand met with agents in New York in January 2019. Thus, he had ample time to prepare for the January 2019 meetings and foreknowledge of topics to be discussed. His false statements in January 2019 were therefore unusually deliberate. And his false statements sought to impede the investigation and prosecution of at least one leading figure (Clark) of a tremendously harmful, impactful website. Weigand apparently hoped that his close confidante, Clark, would avoid the consequences of his actions.

In evaluating the seriousness of Weigand's false statements, it matters why Weigand lied and what Weigand lied about. Silk Road was paradigm-shifting. Silk Road was specifically designed to make it possible to buy and sell massive amounts of contraband, primarily drugs, but to protect the identities of the site's many users. It was extremely sophisticated; it was massive in scope, with more than 1.5 million transactions worldwide worth more than $200 million; it was the first large site to combine various anonymizing technologies; and it caused serious harm. The world still feels Silk Road's impact today through various copycat marketplaces on the dark web, which openly advertise and sell drugs, weapons, malware, and other contraband. It took years of

investigating to determine who was running Silk Road. Weigand's occasional insights about technology, security, and vulnerabilities contributed to Silk Road's success and arguably to its longevity. It is fair to ask the question whether Silk Road would have lasted for as long as it did, and caused as much harm as it did, if not for Weigand's occasional insights. In addition, Silk Road's principals (Ulbricht and Clark) sought to use stunning violence, even murder, to protect their empire. Ulbricht and Clark committed exceptionally serious misconduct worthy of a commensurate punishment. Yet Weigand sought, repeatedly, to help Clark evade consequences for his crimes. As tremendously harmful as Silk Road was, it would be even more so if there were no criminal consequences for its principals—an outcome Weigand apparently hoped to achieve through his false statements.

Our justice system and nation have an extremely strong interest in fair court proceedings; accurate information is the very foundation of just proceedings. Weigand sought to interfere with this process. For instance, in January 2019, Weigand told law enforcement that he knew Clark as "Thomas Clark" and as "Mongoose"; that he had stayed at Clark's home in London; and that he knew that Clark was from the United Kingdom. In other words, Weigand knew Clark so well that he knew Clark's name and had stayed in Clark's home. Yet Weigand also stated that he did *not* know who "Variety Jones" was on Silk Road, but that he knew a user with the moniker "Variety Jones" on PlanetGanja forums who supposedly was from Texas. The implication of Weigand's statements was that "Variety Jones" on Silk Road might be a Texan, but Clark was not a Texan. Weigand's claim not to know the identity of "Variety Jones" on Silk Road—and his pointing in the direction of a Texan—were false statements, but led the Government to make a disclosure to Clark, which could have affected Clark's then-ongoing case.[15] To put the point directly: Weigand was willing to lie, obstruct court proceedings, and go to prison in order to protect Clark, a man who was willing to use violence to protect an online drug empire.

Thus, the nature and circumstances of Weigand's false statements offense—including its seriousness, deception, deliberateness, and intended harmfulness—call for a very serious sentence. Such a sentence is also needed to ensure just punishment and to promote respect for the law.

Second, deterrence interests likewise call for a top-of-the-Guidelines sentence. As to general deterrence, the Government—and the justice system—rely on accurate information in order to make critical determinations. The consequences can be enormously significant (*e.g.*, for defendants, victims, and others) when an individual deliberately injects false information into the justice system's equation. The consequences for such an individual must also be significant. A serious punishment is warranted to send a message to others that such conduct will not be tolerated.

---

[15] Clark explained his monikers to Ulbricht in chats recovered from Ulbricht's laptop, including the following:

> (2012-06-28 17:45) cimon: 10 years ago, I created the nick Variety Jones, and about 6 months later, turned it over to a guy from Texas, who ran with it for 9 years
> (2012-06-28 17:45) cimon: and I took it back to do SR
> (2012-06-28 17:46) cimon: with his permission, as Mongoose name ties to my IRL identity now

As to specific deterrence, Weigand's parade of criminality lasted eight *years*. The sheer volume and variety of his misconduct are troubling; so is the number of missed "stop" signs. First, Weigand and Clark joined Silk Road and hacked Silk Road; and Weigand gave technological advice to Clark and Ulbricht. Then, law enforcement shut down Silk Road. For many individuals, even many criminals, that would have been a wake-up call—a clear sign to stop committing crime. That was not Weigand's reaction, however. Rather, in late 2013, as soon as the Government disclosed that it had been able to access the contents of Ulbricht's laptop, Weigand suddenly traveled to London and removed Silk Road evidence from Clark's apartment, a clear effort to obstruct the investigation. And around the same time, Weigand was carefully laundering Silk Road proceeds through structured, layered transactions over many months. In 2015, Ulbricht was convicted and sentenced to life imprisonment. That should have been another very clear wake-up call—another strong signal to stop committing crime. That was not Weigand's reaction, however. Rather, he and Clark continued their obstructive campaign, culminating in Weigand's lies to law enforcement in 2019. It is clear that a serious sentence is necessary to communicate to this defendant what the various prior stop signs evidently did not.

Third, considerations of relative culpability also support a top-of-the-Guidelines sentence. In the Government's view, there is not a perfect comparator for this defendant. The other Silk Road participants who have been prosecuted to date had more integral involvement in the site on a day-to-day basis than did this defendant. At the same time, none of those individuals waged an approximately eight-year campaign of illegality; and none of those individuals (except Clark) engaged in an extensive obstructive campaign after Silk Road was shuttered. Thus, during the time that Silk Road existed (2011-13), Weigand's misconduct was less pervasive than other prosecuted individuals; but during subsequent years (2013-19), Weigand's misconduct was generally worse, more multifaceted, and more harmful. Accordingly, Weigand is arguably *sui generis* in the realm of Silk Road prosecutions. However, for context, a survey of several Silk Road prosecutions is provided next.

The two most culpable participants in Silk Road were clearly Ulbricht and Clark. (*See* 14 Cr. 68; 15 Cr. 866; *see also* PSR ¶¶ 5-6). Ulbricht and Clark not only shaped Silk Road in every respect, but sought to use violence, even murder, to protect it. Ulbricht was sentenced to life imprisonment, while Clark is currently pending sentence.

Several members of Ulbricht's Silk Road staff—who served as forum moderators, site administrators, etc.—have been sentenced to varying terms of imprisonment, such as 78 months, 66 months, and about 17 months (Gary Davis, Andrew Jones, and Peter Nash, respectively). *See* 13 Cr. 950 (JMF). Jones and Davis served as "site administrators" on Silk Road for about 12 and 4 months, respectively. (After Silk Road was shuttered, Jones and Davis also briefly worked for another dark web market.) As site administrators, Jones and Davis's responsibilities included (1) responding to customer support requests from Silk Road users who needed assistance with their accounts; (2) investigating disputes that arose between vendors and buyers, including reporting findings to Ulbricht; and (3) helping enforce the rules for doing business on Silk Road, such as the rule against "out of escrow" sales—*i.e.*, sellers and buyers arranging payments off the site to avoid paying Silk Road commissions. The site administrators' work was valuable: By resolving disputes between buyers and sellers, or "demoting" vendors who did not follow Silk Road's rules, the site administrators helped Silk Road achieve a scale that Ulbricht could not have achieved on his own.

Meanwhile, Peter Nash was a "forum moderator" on Silk Road from around January 2013 to October 2013.[16] As a forum moderator, Nash helped maintain the Silk Road discussion forums—a part of Silk Road where users could post messages to "discussion threads" concerning various topics related to the site, including how to do business on Silk Road and minimize the risk of detection. Nash regularly responded to questions on the forum from Silk Road users, including advising users on how to evade law enforcement. After their arrests, all three men met with the Government: Nash participated in a successful safety-valve proffer; Davis participated in candid safety-valve proffers; and Jones cooperated with the Government and was prepared to testify against Ulbricht, though his testimony ultimately was not needed. (Jones later committed new crimes while released on bail.) The site administrators (Davis, Jones) were sentenced to 78 and 66 months' imprisonment, while the forum moderator (Nash) was sentenced to about 17 months.

A few factors differentiate Weigand's case from Jones, Davis, and Nash's cases. First, Jones, Davis, and Nash were all formal Silk Road employees; Weigand was not (though, as noted above, Weigand declined payment when Ulbricht offered). Second, Jones, Davis, and Nash all pled guilty to (at least) conspiracy to distribute narcotics, which rendered their Guidelines ranges much higher. Third, despite the utility of their work, Jones, Davis, and Nash's contributions to Silk Road did *not* require skills beyond Ulbricht's ken. Ulbricht could have done their jobs if he had only had more time. By contrast, Weigand possessed something that Ulbricht did not—longstanding technical expertise. Fourth, timing matters. Weigand's primary contribution to Silk Road (during its existence) were his occasional insights about security and technology, including when Silk Road was especially vulnerable in the relatively early-going—a particularly important time. By contrast, Jones, Davis, and Nash helped Ulbricht during the second half of Silk Road's existence, when many of the early programming and security hurdles had already been overcome. In that regard, Weigand helped Silk Road exist, while Jones, Davis, and Nash helped it run smoothly and, to an extent, expand. Fifth, only Weigand engaged in a coordinated obstructive campaign after Silk Road was shut down (though Jones did destroy his own laptop and cash out Bitcoin after Ulbricht's arrest). On the whole, in the Government's view, Weigand is clearly more culpable than was Nash, who received a sentence of time served after about 17 months in custody.

Finally, the defense's arguments for a non-custodial sentence are not persuasive:

- First, the defense notes that this case is Weigand's first contact with the justice system. (Def. Mem. 3). While that is literally true, it is unpersuasive here, given that the defendant engaged in an unusually lengthy, complex, sophisticated, multifaceted campaign of illegality. Moreover, the offense itself shows that repeated contact with the FBI and the IRS, in 2018 and 2019, had no impact on the defendant.

- Second, the defense argues that a 59-year-old is "statistically unlikely to reoffend," (*id.* at 9), but statistical *likelihoods* are far less enlightening than Weigand's established track record: His sixth decade was marked by various felonies, from computer hacking to aiding narcotics distribution to money laundering to making false statements. And when he *knew* the Government was investigating, he obstructed in both 2013 and 2019.

[16] Nash briefly was promoted to the role of a site administrator in May 2013, but after a few weeks, Ulbricht decided to move him back to the role of forum moderator.

- Third, the defense notes that Weigand was not a Silk Road principal or employee. (*Id.* at 8). That is true, and it is part of why his Guidelines range is not driven by the massive weight of Silk Road narcotics. (By contrast, Ulbricht's Guidelines range was life.) Implicit in this defense argument is that Silk Road principals, like Clark, merit greater punishment—which is part of why Weigand's lies to protect Clark were so serious. Moreover, a narrow focus on labels (like "employee") misses the key point: for eight years, Weigand either aided Silk Road, profited from Silk Road, or protected Silk Road.

- Fourth, the defense appears to suggest that Weigand's false statements concerned time-barred conduct (*id.* at 9), but that is at least partially incorrect. As of January 2019, the statute of limitations had not run as to at least one of his felonies—money laundering of Silk Road proceeds—as is reflected in the Plea Agreement's Guidelines calculation. Specifically, Weigand's structured, layered transactions of Silk Road Bitcoin persisted until at least June 2014, and his YubiKey sales continued even after that.

- Fifth, the defense argues that COVID-19 poses especially serious risks to Weigand in light of his age (59) and obesity (*id.* at 11), despite his overall good health (*see* PSR ¶ 80). The pandemic is unprecedented, but the BOP continues to take extraordinary measures to ensure inmate safety, and there is significant reason for optimism with several vaccines recently proven to be highly effective. *See, e.g.*, Elizabeth Cohen, CNN, *Moderna's coronavirus vaccine is 94.5% effective, according to company data*, Nov. 16, 2020 (94.5% effectiveness in a vaccine is "as good as it gets," Dr. Anthony Fauci stated), *available at* https://www.cnn.com/2020/11/16/health/moderna-vaccine-results-coronavirus/index.html (last visited December 11, 2020).

Lastly, many typical arguments for lenience simply are not present here (*e.g.*, youth, impressionability, lack of skills or opportunity, perceived financial need, a one-time or short-term mistake, etc.). Simply put, there is no excuse for the defendant's unusually deliberate, harmful conduct. The sentence requested by the defense would send a very clear, and regrettable, message.

V. CONCLUSION

For the reasons set forth above, the Government respectfully submits that a sentence at the top of the Guidelines range is fair and appropriate in this case.

Respectfully submitted,

AUDREY STRAUSS
Acting United States Attorney
Southern District of New York

By: Michael D. Neff
Michael D. Neff
Assistant United States Attorney
(212) 637-2107

cc: Avrom Robin, Esq. (via ECF)